

STANDARD AGREEMENT FORM FOR PROFESSIONAL SERVICES

The parties' contract comprises this Standard Agreement Form, as well as its referenced Articles and their associated Appendices.

1. Agency Contract Number		2. Contract Title	
3. Vendor Number		4. IRIS GAE Number (if used)	5. Alaska Business License Number
This contract is between the State of Alaska,			
6. Department of Health		Division	hereafter the State, and
7. Contractor hereafter the Contractor			
Address			
<p>8.</p> <p>ARTICLE 1. Appendices: Appendices referred to in this contract and attached to it are considered part of it.</p> <p>ARTICLE 2. Performance of Service:</p> <p>2.1 Appendix A (General Provisions), Articles 1 through 16, governs the performance of services under this contract.</p> <p>2.2 Appendix B sets forth the liability and insurance provisions of this contract.</p> <p>2.3 Appendix C sets forth the services to be performed by the contractor.</p> <p>2.4 Appendix D sets forth the provisions for payment.</p> <p>2.5 Appendix E governs the use of Protected Health Information under this contract.</p> <p>2.6 Appendix F governs overall information security as it applies to HIPAA and HITECH.</p> <p>ARTICLE 3. Period of Performance: The period of performance for this contract begins , and ends .</p> <p>ARTICLE 4. Considerations:</p> <p>4.1 In full consideration of the contractor's performance under this contract, the State shall pay the contractor a sum not to exceed \$ in accordance with the provisions of Appendix D.</p> <p>NOTICE: By signature on this contract, the contractor certifies that neither it nor its principles are not currently debarred, suspended, proposed for debarment, or declared ineligible for award by any federal or other government entity.</p>			
9. CONTRACTOR		<p>11. CERTIFICATION: I certify that the facts herein and on supporting documents are correct, that this voucher constitutes a legal charge against funds and appropriations cited, that sufficient funds are encumbered to pay this obligation, or that there is a sufficient balance in the appropriation cited to cover this obligation. I am aware that to knowingly make or allow false entries or alternations on a public record, or knowingly destroy, mutilate, suppress, conceal, remove or otherwise impair the verity, legibility or availability of a public record constitutes tampering with public records punishable under AS 11.56.815-.820. Other disciplinary action may be taken up to and including dismissal.</p>	
Name of Firm			
Signature of Authorized Representative	Date		
Typed or Printed Name of Authorized Representative			
Title			
10. CONTRACTING AGENCY		Signature of Contracting Agency Head or Designee	Date
Department/Division Health /	Date		
Signature of Project Director		Typed or Printed Name	
Typed or Printed Name of Project Director		Title	
Title			

NOTICE: This contract has no effect until signed by the head of contracting agency or designee.

APPENDIX A

GENERAL PROVISIONS

Article 1. Definitions.

- 1.1 In this contract and appendices, "Project Director" or "Agency Head" or "Procurement Officer" means the person who signs this contract on behalf of the Requesting Agency and includes a successor or authorized representative.
- 1.2 "State Contracting Agency" means the department for which this contract is to be performed and for which the Commissioner or Authorized Designee acted in signing this contract.

Article 2. Inspections and Reports.

- 2.1 The department may inspect, in the manner and at reasonable times it considers appropriate, all the contractor's facilities and activities under this contract.
- 2.2 The contractor shall make progress and other reports in the manner and at the times the department reasonably requires.

Article 3. Disputes.

- 3.1 If the contractor has a claim arising in connection with the contract that it cannot resolve with the State by mutual agreement, it shall pursue the claim, if at all, in accordance with the provisions of AS 36.30.620 – 632.

Article 4. Equal Employment Opportunity.

- 4.1 The contractor may not discriminate against any employee or applicant for employment because of race, religion, color, national origin, or because of age, disability, sex, marital status, changes in marital status, pregnancy or parenthood when the reasonable demands of the position(s) do not require distinction on the basis of age, disability, sex, marital status, changes in marital status, pregnancy, or parenthood. The contractor shall take affirmative action to ensure that the applicants are considered for employment and that employees are treated during employment without unlawful regard to their race, color, religion, national origin, ancestry, disability, age, sex, marital status, changes in marital status, pregnancy or parenthood. This action must include, but need not be limited to, the following: employment, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training including apprenticeship. The contractor shall post in conspicuous places, available to employees and applicants for employment, notices setting out the provisions of this paragraph.
- 4.2 The contractor shall state, in all solicitations or advertisements for employees to work on State of Alaska contract jobs, that it is an equal opportunity employer and that all qualified applicants will receive consideration for employment without regard to race, religion, color, national origin, age, disability, sex, marital status, changes in marital status, pregnancy or parenthood.
- 4.3 The contractor shall send to each labor union or representative of workers with which the contractor has a collective bargaining agreement or other contract or understanding a notice advising the labor union or workers' compensation representative of the contractor's commitments under this article and post copies of the notice in conspicuous places available to all employees and applicants for employment.
- 4.4 The contractor shall include the provisions of this article in every contract, and shall require the inclusion of these provisions in every contract entered into by any of its subcontractors, so that those provisions will be binding upon each subcontractor. For the purpose of including those provisions in any contract or subcontract, as required by this contract, "contractor" and "subcontractor" may be changed to reflect appropriately the name or designation of the parties of the contract or subcontract.
- 4.5 The contractor shall cooperate fully with State efforts which seek to deal with the problem of unlawful discrimination, and with all other State efforts to guarantee fair employment practices under this contract, and promptly comply with all requests and directions from the State Commission for Human Rights or any of its officers or agents relating to prevention of discriminatory employment practices.
- 4.6 Full cooperation in paragraph 4.5 includes, but is not limited to, being a witness in any proceeding involving questions of unlawful discrimination if that is requested by any official or agency of the State of Alaska; permitting employees of the contractor to be witnesses or complainants in any proceeding involving questions of unlawful discrimination, if that is requested by any official or agency of the State of Alaska; participating in meetings; submitting periodic reports on the equal employment aspects of present and future employment; assisting inspection of the contractor's facilities; and promptly complying with all State directives considered essential by any office or agency of the State of Alaska to insure compliance with all federal and State laws, regulations, and policies pertaining to the prevention of discriminatory employment practices.
- 4.7 Failure to perform under this article constitutes a material breach of contract.

Article 5. Termination.

- 5.1 The Procurement Officer, by written notice, may terminate this contract, in whole or in part, when it is in the best interest of the State. In the absence of breach of contract by the contractor, the State is liable only for payment in accordance with the payment provisions of this contract for services rendered before the effective date of termination.

- 5.2 The Procurement Officer may also, by written notice, terminate this contract under Administrative Order 352 if the contractor supports or participates in a boycott of the State of Israel.

Article 6. No Assignment or Delegation.

The contractor may not assign or delegate this contract, or any part of it, or any right to any of the money to be paid under it, except with the written consent of the Project Director and the Agency Head.

Article 7. No Additional Work or Material.

No claim for additional services, not specifically provided in this contract, performed, or furnished by the contractor, will be allowed, nor may the contractor do any work or furnish any material not covered by the contract unless the work or material is ordered in writing by the Project Director and approved by the Agency Head.

Article 8. Independent Contractor.

The contractor and any agents and employees of the contractor act in an independent capacity and are not officers or employees or agents of the State in the performance of this contract.

Article 9. Payment of Taxes.

As a condition of performance of this contract, the contractor shall pay all federal, State, and local taxes incurred by the contractor and shall require their payment by any Subcontractor or any other persons in the performance of this contract. Satisfactory performance of this paragraph is a condition precedent to payment by the State under this contract.

Article 10. Ownership of Documents.

All designs, drawings, specifications, notes, artwork, and other work developed in the performance of this agreement are produced for hire and remain the sole property of the State of Alaska and may be used by the State for any other purpose without additional compensation to the contractor. The contractor agrees not to assert any rights and not to establish any claim under the design patent or copyright laws. Nevertheless, if the contractor does mark such documents with a statement suggesting they are trademarked, copyrighted, or otherwise protected against the State's unencumbered use or distribution, the contractor agrees that this paragraph supersedes any such statement and renders it void. The contractor, for a period of three years after final payment under this contract, agrees to furnish and provide access to all retained materials at the request of the Project Director. Unless otherwise directed by the Project Director, the contractor may retain copies of all the materials.

Article 11. Governing Law; Forum Selection

This contract is governed by the laws of the State of Alaska. To the extent not otherwise governed by Article 3 of this Appendix, any claim concerning this contract shall be brought only in the Superior Court of the State of Alaska and not elsewhere.

Article 12. Conflicting Provisions.

Unless specifically amended and approved by the Department of Law, the terms of this contract supersede any provisions the contractor may seek to add. The contractor may not add additional or different terms to this contract; AS 45.02.207(b)(1). The contractor specifically acknowledges and agrees that, among other things, provisions in any documents it seeks to append hereto that purport to (1) waive the State of Alaska's sovereign immunity, (2) impose indemnification obligations on the State of Alaska, or (3) limit liability of the contractor for acts of contractor negligence, are expressly superseded by this contract and are void.

Article 13. Officials Not to Benefit.

Contractor must comply with all applicable federal or State laws regulating ethical conduct of public officers and employees.

Article 14. Covenant Against Contingent Fees.

The contractor warrants that no person or agency has been employed or retained to solicit or secure this contract upon an agreement or understanding for a commission, percentage, brokerage or contingent fee except employees or agencies maintained by the contractor for the purpose of securing business. For the breach or violation of this warranty, the State may terminate this contract without liability or in its discretion deduct from the contract price or consideration the full amount of the commission, percentage, brokerage or contingent fee.

Article 15. Compliance.

In the performance of this contract, the contractor must comply with all applicable federal, state, and borough regulations, codes, and laws, and be liable for all required insurance, licenses, permits and bonds.

Article 16. Force Majeure:

The parties to this contract are not liable for the consequences of any failure to perform, or default in performing, any of their obligations under this Agreement, if that failure or default is caused by any unforeseeable Force Majeure, beyond the control of, and without the fault or negligence of, the respective party. For the purposes of this Agreement, Force Majeure will mean war (whether declared or not); revolution; invasion; insurrection; riot; civil commotion; sabotage; military or usurped power; lightning; explosion; fire; storm; drought; flood; earthquake; epidemic; quarantine; strikes; acts or restraints of governmental authorities affecting the project or directly or indirectly prohibiting or restricting the furnishing or use of materials or labor required; inability to secure materials, machinery, equipment or labor because of priority, allocation or other regulations of any governmental authorities.

Appendix B

Indemnity and Insurance

Article 1. Indemnification

The contractor shall indemnify, hold harmless, and defend the contracting agency from and against any claim of, or liability for error, omission or negligent act of the contractor under this agreement. The contractor shall not be required to indemnify the contracting agency for a claim of, or liability for, the independent negligence of the contracting agency. If there is a claim of, or liability for, the joint negligent error or omission of the contractor and the independent negligence of the contracting agency, the indemnification and hold harmless obligation shall be apportioned on a comparative fault basis. "Contractor" and "contracting agency", as used within this and the following article, include the employees, agents and other contractors who are directly responsible, respectively, to each. The term "independent negligence" is negligence other than in the contracting agency's selection, administration, monitoring, or controlling of the contractor and in approving or accepting the Contractor's work.

Article 2. Insurance

Without limiting contractor's indemnification, it is agreed that contractor shall purchase at its own expense and maintain in force at all times during the performance of services under this agreement the following policies of insurance. Where specific limits are shown, it is understood that they shall be the minimum acceptable limits. If the contractor's policy contains higher limits, the state shall be entitled to coverage to the extent of such higher limits. Certificates of Insurance must be furnished to the contracting officer prior to beginning work and must provide for a notice of cancellation, non-renewal, or material change of conditions in accordance with policy provisions. Failure to furnish satisfactory evidence of insurance or lapse of the policy is a material breach of this contract and shall be grounds for termination of the contractor's services. All insurance policies shall comply with and be issued by insurers licensed to transact the business of insurance under AS 21.

2.1 Workers' Compensation Insurance: The contractor shall provide and maintain, for all employees engaged in work under this contract, coverage as required by AS 23.30.045, and; where applicable, any other statutory obligations including but not limited to Federal U.S.L. & H. and Jones Act requirements. The policy must waive subrogation against the State.

2.2 Commercial General Liability Insurance: covering all business premises and operations used by the Contractor in the performance of services under this agreement with minimum coverage limits of \$300,000 combined single limit per claim.

2.3 Commercial Automobile Liability Insurance: covering all vehicles used by the contractor in the performance of services under this agreement with minimum coverage limits of \$300,000 combined single limit per claim.

2.4 Professional Liability Insurance: covering all errors, omissions or negligent acts in the performance of professional services under this agreement with minimum coverage limits of \$300,000 per claim /annual aggregate.

Appendix C

Description of Services

Scope of Work

Deliverables

Appendix D

Payment for Services

Payment for services provided shall not exceed \$XXX,000.00 for the initial period of performance of this contract.

The contractor shall bill ...

State Approved Travel Guidelines:

The State will cover costs associated with pre-approved travel per the criteria listed below. Expenses above these criteria must be approved in advance by the Program Manager.

- **Air Travel:** copies of receipts and boarding passes for flights must be submitted with the invoice. The State will reimburse for coach travel only.
 - **Hotel:** copies of original hotel receipts at commercial facilities must be submitted with the invoice. Actual lodging expenses that exceed \$300 room rate per night, excluding taxes, must be approved in advance by the Program Manager.
 - **Rental Car:** copies of the rental car receipt and agreement must be submitted with the invoice. Rental should be for a mid-size or less car (unless approved in advance) and the rental period is to cover the business travel period only.
 - **Ground Transportation:** between the Contractor's home and the airport, and the destination airport and hotel; via airport shuttle, courtesy van, or taxi service.
 - **Per Diem:** the maximum amount for food and all other travel related incidentals in Alaska is \$60 per day, per person.
- Note:** Costs of parking violations will not be reimbursed.

Invoicing

The contractor will submit monthly invoices detailing services performed in accordance with Appendix C.

The invoice must:

- Reference the contractor's name, address and phone number
- Reference the contract number: 1624-0xx
- Include an invoice number
- Reference the Department of Health, Division of
- Itemize the contractual services provided during the period invoiced as described in Appendix C

The contractor shall submit invoices to the address specified below no later than 30 days after the end the period for which services were performed. Failure to include the required information on the invoice may cause an unavoidable delay to the payment process. The State will pay all invoices within thirty (30) days of invoice approval by the Project Director.

Email invoices to:

[\[division email\]@alaska.gov](mailto:[division email]@alaska.gov)

(please reference the contract in the subject line)

Notwithstanding any other provision of this contract, it is understood and agreed that the State shall withhold payment at any time the contractor fails to perform work as required under this contract.

APPENDIX E
STATE OF ALASKA DEPARTMENT OF HEALTH
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA")
BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement is between the State of Alaska, Department of Health ("Covered Entity" or "CE") and the Contractor ("Business Associate" or "BA").

RECITALS

Whereas,

- A. CE wishes to disclose certain information to BA, some of which may constitute Protected Health Information ("PHI");
- B. It is the goal of CE and BA to protect the privacy and provide for the security of PHI owned by CE that is disclosed to BA or accessed, received, stored, maintained, modified or retained by BA in compliance with HIPAA (42 U.S.C. 1320d – 3120d-8) and its implementing regulations at 45 C.F.R. 160 and 45 C.F.R. 164 (the "Privacy and Security Rule"), the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5) (the "HITECH Act"), and with other applicable laws;
- C. The purpose and goal of the HIPAA Business Associate Agreement ("BAA") is to satisfy certain standards and requirements of HIPAA, HITECH Act, and the Privacy and Security Rule, including but not limited to 45 C.F.R. 164.502(e) and 45 C.F.R. 164.504(e), as may be amended from time to time;
- D. CE may operate a drug and alcohol treatment program that must comply with the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations, 42 U.S.C. 290dd-2 and 42 C.F.R. Part 2 (collectively "Part 2"); and
- E. BA may be a Qualified Service Organization ("QSO") under Part 2 and therefore must agree to certain mandatory provisions regarding the use and disclosure of substance abuse treatment information.

Therefore, in consideration of mutual promises below and the exchange of information pursuant to the BAA, CE and BA agree as follows:

1. Definitions.

- a. General: As used in this BAA, the terms "Protected Health Information," "Health Care Operations," and other capitalized terms have the same meaning given to those terms by HIPAA, the HITECH Act and the Privacy and Security Rule. In the event of any conflict between the mandatory provisions of HIPAA, the HITECH Act or the Privacy and Security Rule, and the provisions of this BAA, HIPAA, the HITECH Act or the Privacy and Security Rule shall control. Where the provisions of this BAA differ from those mandated by HIPAA, the HITECH Act or the Privacy and Security Rule but are nonetheless permitted by HIPAA, the HITECH Act or the Privacy and Security Rule, the provisions of the BAA shall control.
- b. Specific:
 - 1) Business Associate: "Business Associate" or "BA" shall generally have the same meaning as the term "business associate" at 45 C.F.R. 160.103.
 - 2) Covered Entity: "Covered Entity" or "CE" shall have the same meaning as the term "covered entity" at 45 C.F.R. 160.103.
 - 3) Privacy and Security Rule: "Privacy and Security Rule" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

4) Triennially: “Triennially” shall mean once every three years.

2. Statement of Work and Responsibilities.

As provided by AS 44.21.020 and AS 44.21.160, The BA provides automatic data processing services to the CE. These services include storage, transmission, security, and recovery of electronic information owned by CE. BA is responsible for ensuring continuity of service, delivery, and access to CE electronic information at all times including in the event of a disaster.

3. Permitted Uses and Disclosures by Business Associate.

a. BA may only use or disclose PHI for the following purposes:

- 1) BA may use or disclose PHI as required by law.
- 2) BA agrees to make uses and disclosures and requests for PHI consistent with CE’s minimum necessary policies and procedures.
- 3) BA may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by CE, except for the specific uses and disclosures set out below.
- 4) BA may disclose PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA, provided the disclosures are required by law, or BA obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notified BA of any instances of which it is aware in which the confidentiality of the information has been breached.
- 5) BA may provide data aggregation services related to the health care operations of CE.

4. Obligations of Business Associate.

a. Permitted uses and disclosures: BA may only use and disclose PHI owned by the CE that it creates, receives, maintains, or transmits if the use or disclosure is in compliance with each applicable requirement of 45 C.F.R. 164.504(e) of the Privacy Rule or this BAA. The additional requirements of Subtitle D of the HITECH Act contained in Public Law 111-5 that relate to privacy and that are made applicable with respect to Covered Entities shall also be applicable to BA and are incorporated into this BAA.

To the extent that BA discloses CE’s PHI to a subcontractor, BA must obtain, prior to making any such disclosure: (1) reasonable assurances from the subcontractor that it will agree to the same restrictions, conditions, and requirements that apply to the BA with respect to such information; and (2) an agreement from the subcontractor to notify BA of any Breach of confidentiality, or security incident, within three business days of when it becomes aware of such Breach or incident.

b. Safeguards: 45 C.F.R. 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures, and documentation requirements) shall apply to BA in the same manner that such sections apply to CE, and shall be implemented in accordance with HIPAA, the HITECH Act, and the Privacy and Security Rule. The additional requirements of Title XIII of the HITECH Act contained in Public Law 111-5 that relate to security and that are made applicable to Covered Entities shall also apply to BA and are incorporated into this BAA.

Unless CE agrees in writing that this requirement is infeasible with respect to certain data, BA shall secure all paper and electronic PHI by encryption or destruction such that the PHI is rendered unusable, unreadable or indecipherable to unauthorized individuals; or secure paper, film and electronic PHI in a manner that is consistent with guidance issued by the Secretary of the United States Department of Health and Human

Services specifying the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals, including the use of standards developed under Section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by Section 13101 of the HITECH Act contained in Public Law 111-5.

BA shall not use personally owned devices to create, receive, maintain, or transmit PHI. Devices the BA uses to create, receive, maintain, or transmit CE's electronic PHI shall be owned and managed by BA or CE.

BA shall patch its operating systems and all applications within two weeks of the release of any patch. BA shall keep its antivirus and antimalware installed and active. BA shall limit its use of administrative accounts for necessary IT operations only.

- c. Reporting Unauthorized Disclosures and Breaches: During the term of this BAA, BA shall notify CE within 72 hours of discovering a Breach of security; intrusion; or unauthorized acquisition, access, use or disclosure of CE's PHI in violation of any applicable federal or state law, including security incidents. BA shall identify for the CE the individuals whose unsecured PHI has been, or is reasonably believed to have been, breached so that CE can comply with any notification requirements if necessary. BA shall also indicate whether the PHI subject to the Breach; intrusion; or unauthorized acquisition, access, use, or disclosure was encrypted or destroyed at the time. BA shall take prompt corrective action to cure any deficiencies that result in Breaches of security; intrusion; or unauthorized acquisition, access, use, and disclosure. BA shall fulfill all breach notice requirements unless CE notifies BA that CE will take over the notice requirements. BA shall reimburse CE for all costs incurred by CE that are associated with any mitigation, investigation and notice of Breach CE undertakes or provides under HIPAA, HITECH Act, and the Privacy and Security Rule as a result of a Breach of CE's PHI caused by BA or BA's subcontractor or agent.

If the unauthorized acquisition, access, use or disclosure of CE's PHI involves only Secured PHI, BA shall notify CE within 10 days of discovering the Breach but is not required to notify CE of the names of the individuals affected.

- d. BA is not an agent of CE.
- e. BA's Agents: If BA uses a subcontractor or agent to provide services under this BAA, and the subcontractor or agent creates, receives, maintains, or transmits CE's PHI, the subcontractor or agent shall sign an agreement with BA containing substantially the same provisions as this BAA and further identifying CE as a third-party beneficiary with rights of enforcement and indemnification from the subcontractor or agent in the event of any violation of the subcontractor or agent agreement. BA shall mitigate the effects of any violation of that agreement.
- f. Availability of Information to CE: Within 15 days after the date of a written request by CE, BA shall provide any information necessary to fulfill CE's obligations to provide access to PHI under HIPAA, the HITECH Act, or the Privacy and Security Rule.
- g. Accountability of Disclosures: If BA is required by HIPAA, the HITECH Act, or the Privacy or Security Rule to document a disclosure of PHI, BA shall make that documentation. If CE is required to document a disclosure of PHI made by BA, BA shall assist CE in documenting disclosures of PHI made by BA so that CE may respond to a request for an accounting in accordance with HIPAA, the HITECH Act, and the Privacy and Security Rule. Accounting records shall include the date of the disclosure, the name and if known, the address of the recipient of the PHI, the name of the individual who is subject of the PHI, a brief description of the PHI disclosed and the purpose of the disclosure. Within 15 days of a written request by CE, BA shall make the accounting record available to CE.
- h. Amendment of PHI: Within 30 days of a written request by CE, BA shall amend PHI maintained, transmitted, created, or received by BA on behalf of CE as directed by CE when required by HIPAA, the HITECH Act or the

Privacy and Security Rule, or take other measures as necessary to satisfy CE's obligations under 45 C.F.R. 164.526.

- i. Internal Practices: BA shall make its internal practices, books and records relating to the use and disclosure of CE's PHI available to CE and all appropriate federal agencies to determine CE's and BA's compliance with HIPAA, the HITECH Act and the Privacy and Security Rule.
- j. Risk Assessment: Upon agreement execution and triennially thereafter, or upon changes that occur which significantly affect the security posture of the system (whichever comes first), BA shall comply and complete CE's security assessment. Upon receipt of the security assessment, CE will review BA's responses prior to granting authority to operate, and provide any necessary instruction to ensure the confidentiality, integrity, and availability of CE's PHI. BA shall triennially, or upon changes that occur which significantly affect the security posture of the system (whichever comes first), review and update CE security assessment, as required, in order to comply with BA's current system controls. BA must provide an implementation response for each specific system control. Upon receipt of the updated assessment, CE will review the changes to the system for renewal of authority to operate.
- k. To the extent BA is to carry out one or more of CE's obligations under Subpart E of 45 C.F.R. Part 164, BA must comply with the requirements of that Subpart that apply to CE in the performance of such obligations.
- l. Audits, Inspection and Enforcement: CE may, after providing 10 days' notice to the BA, conduct an inspection of the facilities, systems, books, logs, and records of BA that relate to BA's use of CE's PHI, including inspecting logs showing the creation, modification, viewing, and deleting of PHI at BA's level. Failure by CE to inspect does not waive any rights of the CE or relieve BA of its responsibility to comply with this BAA. CE's failure to detect or failure to require remediation does not constitute acceptance of any practice or waive any rights of CE to enforce this BAA.

Notwithstanding BA's obligation to report under paragraph 3.c of this BAA, BA shall provide a monthly report to CE detailing the unauthorized, or reasonable belief of unauthorized, acquisition, access, use, or disclosure of CE's PHI, including any unauthorized creation, modification, or destruction of PHI and unauthorized login attempts. BA shall include privileged and nonprivileged accounts in its audit and report, indicating the unique individual using the privileged account. BA shall also indicate whether CE's PHI subject to unauthorized activity was encrypted or destroyed at the time of the unauthorized activity.

BA shall provide a yearly report to CE that lists the names of all individuals with technical or physical access to CE's PHI and the scope of that access.

- m. Restrictions and Confidential Communications: Within 10 business days of notice by CE of a restriction upon use or disclosure or request for confidential communications pursuant to 45 C.F.R.164.522, BA shall restrict the use or disclosure of an individual's PHI. BA may not respond directly to an individual's request to restrict the use or disclosure of PHI or to send all communication of PHI to an alternate address. BA shall refer such requests to the CE so that the CE can coordinate and prepare a timely response to the requesting individual and provide direction to the BA.
 - n. Indemnification: BA shall indemnify and hold harmless CE for any civil or criminal monetary penalty or fine imposed on CE for acts or omissions in violation of HIPAA, the HITECH Act, or the Privacy or Security Rule that are committed by BA, a member of its workforce, its agent, or its subcontractor.
5. Obligations of CE. CE will be responsible for using legally appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to BA under the BAA until the PHI is received by BA. CE will not request BA to use or disclose PHI in any manner that would not be permissible under HIPAA, the HITECH Act or the Privacy and Security Rule if done by CE.

6. Termination.

- a. Breach: A breach of a material term of the BAA by BA that is not cured within a reasonable period of time will provide grounds for the immediate termination of the contract.
- b. Reasonable Steps to Cure: In accordance with 45 C.F.R. 164.504(e)(1)(ii), CE and BA agree that, if it knows of a pattern of activity or practice of the other party that constitutes a material breach or violation of the other party's obligation under the BAA, the nonbreaching party will take reasonable steps to get the breaching party to cure the breach or end the violation and, if the steps taken are unsuccessful, terminate the BAA if feasible, and if not feasible, report the problem to the Secretary of the U.S. Department of Health and Human Services.
- c. Effect of Termination: Upon termination of the contract, BA will, at the direction of the CE, either return or destroy all PHI received from CE or created, maintained, or transmitted on CE's behalf by BA in any form. Unless otherwise directed, BA is prohibited from retaining any copies of PHI received from CE or created, maintained, or transmitted by BA on behalf of CE. If destruction or return of PHI is not feasible, BA must continue to extend the protections of this BAA to PHI and limit the further use and disclosure of the PHI. The obligations in this BAA shall continue until all of the PHI provided by CE to BA is either destroyed or returned to CE.

7. Amendment. The parties acknowledge that state and federal laws relating to electronic data security and privacy are evolving, and that the parties may be required to further amend this BAA to ensure compliance with applicable changes in law. Upon receipt of a notification from CE that an applicable change in law affecting this BAA has occurred, BA will promptly agree to enter into negotiations with CE to amend this BAA to ensure compliance with changes in law.

8. Ownership of PHI. For purposes of this BAA, CE owns the data that contains the PHI it transmits to BA or that BA receives, creates, maintains, or transmits on behalf of CE.

9. Litigation Assistance. Except when it would constitute a direct conflict of interest for BA, BA will make itself available to assist CE in any administrative or judicial proceeding by testifying as witness as to an alleged violation of HIPAA, the HITECH Act, the Privacy or Security Rule, or other law relating to security or privacy.

10. Regulatory References. Any reference in this BAA to federal or state law means the section that is in effect or as amended.

11. Interpretation. This BAA shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy and Security Rule and applicable state and federal laws. The parties agree that any ambiguity in BAA will be resolved in favor of a meaning that permits the CE to comply with and be consistent with HIPAA, the HITECH Act, and the Privacy and Security Rule. The parties further agree that where this BAA conflicts with a contemporaneously executed confidentiality agreement between the parties, this BAA controls.

12. No Private Right of Action Created. This BAA does not create any right of action or benefits for individuals whose PHI is disclosed in violation of HIPAA, the HITECH Act, the Privacy and Security Rule or other law relating to security or privacy.

13. Privacy and Security Point of Contact. All communications occurring because of this BAA shall be sent to doh.its.dso@alaska.gov in addition to the CE.

In witness thereof, the parties hereto have duly executed this BAA as of the effective date of this contract.

Appendix F
State of Alaska, Department of Health
HIPAA AND HITECH Information Security Agreement (ISA)

This agreement, effective upon the date of full contract execution, is entered into by and between the **Department of Health** (hereafter known as **Covered Entity**) and the **Contractor Name** (hereafter known as **Business Associate**). This agreement is in accordance with **Covered Entity's** obligations under:

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the applicable requirements of HIPAA's implementing regulations issued by the U.S. Department of Health and Human Services (HHS), Title 45 of the Code of Federal Regulations ("C.F.R.") Parts 160-164 ("HIPAA Regulations");
- The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), as incorporated in the American Recovery and Reinvestment Act of 2009, Public Law 111-005;
- The Genetic Information Nondiscrimination Act ("GINA");
- The HIPAA Final Rule (the "Final Rule").

Covered Entity and **Business Associate** acknowledge and agree to the terms and conditions of this agreement to ensure the confidentiality, integrity, and availability of Protected Health Information by lawfully complying with the abovementioned provisions and regulations, all as amended from time to time.

A. Definitions

1. **"Breach"** shall mean the impermissible acquisition, access, use, or disclosure of Protected Health Information (PHI) which compromises the security, confidentiality, privacy, or integrity of such information pursuant to the HITECH Act § 13400, any regulations issued there under, or as amended by law. An impermissible use or disclosure of protected health information is presumed to be a breach unless the **Covered Entity** or **Business Associate**, as applicable, demonstrates that there is a low probability that the protected health information has been compromised. This does not include:
 - a. Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a **Covered Entity** or **Business Associate**, if access was in good faith and within the scope of authority; or
 - b. Inadvertent disclosure by a person authorized to access the PHI to another person authorized to access the PHI.
2. **"Business Associate"** shall mean an individual or entity who or which performs a function or activity on behalf of, or provides a service, to **Covered Entity** that involves the creation, use, or disclosure of PHI. Shall have the meaning given to such term under the HIPAA Privacy Rule, the HIPAA Security Rule, and the HITECH Act, but not limited to, Section 13400 and Section 13401 of the HITECH Act, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103.
3. **"Covered Entity"** shall mean a health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA Regulations. **Covered Entity** shall have the meaning given to such term under the HIPAA Privacy Rule and the HIPAA Security Rule, including but not limited to, 45 C.F.R. Section 160.103.
4. **"Data Aggregation"** shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR Section 164.501.
5. **"Data Breach Notification Rule"** shall mean the standards for Breach Notification of Unsecured Protected Health Information at 45 CFR part 164, subpart D, as amended.
6. **"Designated Record Set"** shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR Section 164.501.
7. **"Electronic Protected Health Information"(ePHI)** shall mean PHI maintained or transmitted in electronic form.

8. **"Health Care Operations"** shall have the meaning as defined under the HIPAA Rules, including, but not limited to, 45 CFR Section 164.501.
9. **"Individual"** shall have the meaning as defined in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
10. **"Limited Data Set"** shall mean PHI that excludes direct identifiers of the individual or of relatives, employers, or household members of the individual. (See 45 C.F.R. § 164.514(e)(2)).
11. **"Minimum Necessary". Business Associate** shall only request, use, and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure.
12. **"Personally Identifiable Information"** (PII), as defined in OMB Memorandum M-07-16 refers to "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or associated with a specific individual." The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.
13. **"Privacy Official"** shall mean the **Covered Entity's** designated individual, and such individual's designees, who are responsible for the development and implementation of **Covered Entity's** policies and procedures regarding privacy and confidentiality of PHI.
14. **"Protected Health Information"** (PHI) shall mean either medical information or personally identifiable information in electronic, physical, or oral form. Medical information is any information in possession of, or derived from, a physician or other provider of health care, or a health care service plan regarding an individual's medical history, mental or physical condition, or treatment. PHI shall have the meaning given to such term under the HIPAA Privacy Rule and the GINA, including, but not limited to 45 C.F.R. Sections 160.103.
15. **"Required by law"** shall have the meaning given to such term as stated within 45 C.F.R. §164.103.
16. **"Security Incident"** shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system that is created, received, maintained, or transmitted by or on behalf of **Covered Entity**. (See 45 C.F.R. §164.304).
17. **"Unsecured PHI"** shall mean PHI that is not secured in accordance with guidance issued by the United States Department of Health and Human Services (HHS) under the HITECH Act including, but not limited to, 42 U.S.C. Section 17932(h), and applicable regulations issued thereunder.

B. Privacy and Security of PHI

1. **Permitted Uses and Disclosures.** **Business Associate** is permitted or required to use or disclose PHI it creates, receives, maintains, or transmits in service to **Covered Entity** only as follows:
 - a. **Functions and Activities on Covered Entity's Behalf.** **Business Associate** is permitted to use and disclose the minimum necessary PHI it creates, receives, maintains, or transmits to/from **Covered Entity**, to perform those services set forth in the underlying contract, provided that no such use or disclosure would violate HIPAA Regulations, or the HITECH Act and applicable regulations issued thereunder, if **Covered Entity** itself made the use or disclosure.
 - b. **Marketing and Fundraising.** Unless expressly authorized by the underlying contract between the parties, **Business Associate** shall not Use or Disclose PHI for any marketing or fundraising purpose.
 - c. **Audit.** For purposes of determining **Business Associate's** compliance with HIPAA, upon request of **Covered Entity** or the Secretary of HHS, **Business Associate** shall:
 - i. Make its HIPAA policies and procedures, related documentation, records maintained, and any other relevant internal practices, books, and records relating to the use and disclosure of PHI, available to the Secretary of HHS or to **Covered Entity**.
 - ii. Provide reasonable access to **Business Associate's** facilities, equipment, hardware, and software used for the maintenance or processing of **Covered Entity's** PHI.

- d. **Record Keeping.** Business Associate agrees to implement appropriate record keeping procedures to enable it to comply, and to adequately evidence such compliance, including; the documentation required regarding subcontractors and agents, records of Business Associate's workforce HIPAA education and training, documentation related to any breach, Business Associate Agreements issued to third parties with whom Business Associate discloses PHI for Business Associate's proper management and administration, or as required by law.
 - e. **Business Associate's Operations.** Business Associate may use and disclose the PHI it creates, receives, maintains, or transmits in service to **Covered Entity**, as necessary, to perform the Business Associate's obligations under the contract, to enable that Business Associate's proper management and administration of **Covered Entity's** PHI, or to carry out Business Associate's legal responsibilities. All PHI disclosures must maintain compliance with the HIPAA minimum necessary standard.
2. **Prohibition on Unauthorized Use or Disclosure.** **Business Associate** shall neither use nor disclose PHI it creates, receives, maintains, or transmits in service to **Covered Entity**, except as permitted or required by the contract, as required by law, or as otherwise permitted in writing by **Covered Entity**. **Business Associate** acknowledges that **Business Associate** will be liable for violating any of the requirements of this agreement relating to the use or disclosure of PHI, or any privacy-related requirements of the HITECH Act and regulations issued thereunder.
3. **Offshoring Prohibition.** **Business Associate** may not transmit or make PHI accessible to any recipient outside the United States of America without **Covered Entity's** prior written consent.
4. **Compliance with Laws; Regulatory Amendments.** **Business Associate** shall comply with all applicable state and federal privacy and security laws pursuant to HIPAA, HIPAA Regulations, the HITECH Act, and any regulations promulgated thereunder. Any regulations or amendments to applicable privacy and security laws shall be automatically included in this a, such that this agreement remains in compliance with such regulations or amendments. Any future state privacy and security laws shall be automatically included in this agreement, such that this agreement remains in compliance with such regulations or amendments.
5. **Effect.** The terms and provisions of this agreement shall supersede any other conflicting or inconsistent terms and provisions in any other contract between the parties, including any exhibits, attachments, addenda, or amendments thereto, and any other documents incorporated by reference therein, which pertain or relate to the use or disclosure of PHI by either party, or the creation or receipt of PHI by **Business Associate** on behalf of **Covered Entity**.
6. **Change in Law Amendments.** The parties agree to amend this agreement to the extent necessary to allow either arty to comply with any amendments to any provision of HIPAA or its implementing regulations or any judicial, legislative, or administrative interpretation which alters or conflicts with any provisions contained herein.
7. **Definitions, Construction of Terms, and Interpretation.** Capitalized terms herein without definition shall have the same meanings assigned to such terms in 45 CFR Parts 160 and 164. The terms of this agreement shall be construed in light of any applicable interpretation or guidance on HIPAA and/or the Privacy and Security Standards issued by HHS or the Office for Civil Rights from time to time. This agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and the Privacy and Security Standards. The parties agree that any ambiguity in this agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the Privacy and Security Standards.
8. **No Third-Party Beneficiaries.** Nothing in this agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
9. **Independent Contractors.** The parties agree that they are independent parties and not employees, partners, or party to a joint venture of any kind. Neither party shall hold itself out as the other's agent for any purpose and shall have no authority to bind the other to any obligation.

10. **Information Safeguards.** **Business Associate** shall develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards, in compliance with applicable state and federal laws, to preserve the integrity, confidentiality, and availability of PHI, and to prevent unauthorized disclosures of PHI created or received for or from **Covered Entity** as required by 45 C.F.R. Part 164, Subpart C, the HITECH Act, HHS' guidance on the Direct Liability of Business Associates, and any applicable regulations issued thereunder. **Business Associate** shall document and keep such safeguards current and shall develop and implement policies and procedures to meet the Security Rule documentation requirements of the HITECH Act and shall, upon **Covered Entity's** request, either orally or in writing, provide **Covered Entity** with a copy of its policies and procedures related to such safeguards. **Business Associate** shall also provide reasonable description of the practices and processes that are in place to support the policies, procedures, and requirements.
 - a. 45 C.F.R. 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures, and documentation requirements) shall apply to **Business Associate** in the same manner that such sections apply to **Covered Entity** and shall be implemented in accordance with HIPAA, the HITECH Act, and the Privacy and Security Rule. The additional requirements of Title XIII of the HITECH Act contained in Public Law 111-5 that relate to security and that are made applicable to **Covered Entity** shall also apply to **Business Associate** and are incorporated into this Information Security Agreement.
11. **Subcontractors and Agents.** **Business Associate** shall require any of its subcontractors and agents to which **Business Associate** is permitted by this agreement or in writing by **Covered Entity** to disclose PHI, to sign a further Business Associate Agreement and to provide reasonable assurance evidenced by written contract, that such subcontractor or agent shall comply with the same privacy and security safeguard obligations with respect to PHI that are applicable to **Business Associate** under this agreement, including, but not limited to:
 - a. Holding such PHI in confidence and using or further disclosing it only for the purpose for which **Business Associate** disclosed it to the agent, subcontractor, or other third party, or as required by law.
 - b. In compliance with 45 CFR §§ 164.400-414 **Subcontractor** or **Agent** shall provide notification to **Business Associate**, and the **Business Associate** shall provide notification to the **Covered Entity**, of any instance of which the agent, subcontractor, or other third party becomes aware in which the confidentiality of such PHI was breached.
12. **Minimum Necessary and Limited Data Set.** **Business Associate's** use, disclosure, or request of PHI shall utilize a limited data set, whenever possible. Otherwise, **Business Associate** shall, in its performance of the functions, activities, services, and operations specified in Section B.1 above, make reasonable efforts to use, to disclose, and to request only the minimum amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure, or request, except that **Business Associate** shall not be obligated to comply with the minimum necessary limitations with respect to those exceptions specified in 45 C.F.R. § 164.502 (b)(2). **Business Associate** shall comply with the requirements governing the minimum necessary use and disclosure of PHI set forth in the HITECH Act § 13405(b) and any applicable regulations or other guidance issued thereunder.
13. **Employee Education.** **Business Associate** shall inform all of its employees, workforce members, subcontractors, and agents ("**Business Associate** Personnel"), whose services may be used to satisfy **Business Associate's** obligations under the agreement, of the **Business Associate's** obligations under this agreement. **Business Associate** represents and warrants that the **Business Associate** Personnel are under legal obligation to **Business Associate**, by contract or otherwise, sufficient to enable **Business Associate** to fully comply with the provisions of this agreement. **Business Associate** will maintain a system of sanctions for any **Business Associate** Personnel who violates this agreement.
14. **Risk Assessment.** Upon agreement execution, and prior to any system entering a production state or containing production data, **Business Associate** must complete **Covered Entity's** established security

assessment process and obtain Authority to Operate (ATO). Any identified risks must be remediated to ensure that the system complies with the **Covered Entity's** security standards and the **Covered Entity's** selected standards for HIPAA compliance. This security assessment process must be updated and reassessed triennially thereafter, or upon changes that occur which significantly affect the security posture of the system (whichever comes first), and Authority to Operate must be updated to reflect the current risk profile of the system.

C. PHI Access, Amendment, Restriction, and Reporting

1. **Access.** **Business Associate** shall, upon **Covered Entity's** reasonable request, and in compliance with 45 CFR 164.524(b)(2)(i), permit an individual (or the individual's personal representative) to obtain and inspect copies of any PHI about the individual which **Business Associate** created or received for or from **Covered Entity** and that is in **Business Associate's** custody or control. **Business Associate** shall provide such information in an electronic format, if requested by the individual, and as directed by **Covered Entity**.
2. **Amendment.** **Business Associate** shall, upon receipt of notice from **Covered Entity**, promptly amend or permit **Covered Entity** access to amend, any portion of an individual's PHI which **Business Associate** created or received for or from **Covered Entity** and that is in **Business Associate's** custody or control.
3. **Restriction.** **Business Associate** shall, upon **Covered Entity's** written notice of any changes in, or restrictions to, the permitted use or disclosure of PHI, promptly restrict the use or disclosure of PHI consistent with the **Covered Entity's** instructions. **Covered Entity** will promptly notify **Business Associate** in writing of the termination of any such restriction agreement and, with respect to termination of any such restriction agreement, instruct **Business Associate** as to whether any PHI will remain subject to the terms of the restriction agreement.
4. **Reporting.**
 - a. Legal or Authorized Disclosure Reporting. Except as permitted by applicable law, **Business Associate** shall document each disclosure it makes of an individual's PHI to a third party. Such report shall include the affected individual's name, the person or entity to whom the PHI was disclosed, what was disclosed, why the information was disclosed, the date of such disclosure and any other information necessary for **Covered Entity** to comply with relevant statutes and regulations. Such report shall be furnished to **Covered Entity** within ten (10) calendar days of its request. In addition, where **Business Associate** is contacted directly by an individual based on information provided to the individual by **Covered Entity**, and where so required by the HITECH Act and/or any accompanying regulations, **Business Associate** shall make such report available directly to the individual.
 - i. **Disclosure Accounting.** Upon request, **Business Associate** shall forward to **Covered Entity** a report of disclosures as required by 45 C.F.R. § 164.528, and as applicable, the HITECH Act § 13405(c) and any regulations issued thereunder.
 - ii. **Disclosure Accounting Retention.** **Business Associate** shall maintain an accounting of such disclosures for six (6) years after the date of occurrence.
 - b. **Security Incident Reporting.** **Business Associate** shall report to **Covered Entity's** Chief Privacy Officer and Chief Information Security Officer as stipulated in 45 CFR 164.410 after **Business Associate** knows, or should reasonably have known of such Security Incident, any Security Incident of which **Business Associate** becomes aware. In addition, **Business Associate** shall, upon **Covered Entity's** request, report any attempted unauthorized access, use, disclosure, modification, or destruction of ePHI. If any such security incident resulted in a disclosure of PHI not permitted by this agreement, **Business Associate** shall make a report in accordance with Section C.5(c), below. If **Business Associate** is aware of a pattern of activity or practice by its subcontractor that constitutes a breach or violation of the subcontractor's obligations under its Business Associate Agreement or obligations with **Business Associate**, **Business Associate** must take reasonable steps to cure the breach or end the violation and take further actions consistent with 45 C.F.R. § 164.504.

- c. **Breach Reporting.** **Business Associate** shall report to **Covered Entity** any breaches of PHI as stipulated in 45 CFR 164.410. **Business Associate** shall make such report to **Covered Entity's** Privacy Officer after **Business Associate** knows, or should reasonably have known, of such breach. **Business Associate** shall cooperate with **Covered Entity** in investigating such breach, and in meeting **Covered Entity's** obligations under the HITECH Act and any other security breach notification laws. **Business Associate** shall report all breaches to **Covered Entity** in writing (and in the format requested by **Covered Entity**) and such reports shall, at a minimum:
- i. Identify the nature of the breach, including the date of the breach and the date of discovery of the breach.
 - ii. Identify which elements of the PHI (e.g., full name, social security number, date of birth, etc.) were breached, or were part of the breach.
 - iii. Identify who was responsible for the breach and who received the PHI.
 - iv. Identify what corrective actions **Business Associate** took or will take to prevent further incidents of a breach.
 - v. Identify what **Business Associate** did or will do to mitigate any deleterious effect of the breach.
 - vi. Identify **Business Associate** contact information and procedures to enable **Covered Entity** to obtain additional information if required.
 - vii. Provide such other information, including a written report, as **Covered Entity** may reasonably request.
- d. **Obligations in the Event of an Improper Pattern of Activity or Practice.** In the event that either party becomes aware of a pattern of activity or practice of the other party that constitutes a material breach or violation of this agreement, the party discovering such pattern of activity or practice must take reasonable steps to cause the other party to cure the breach or end the violation. If a cure is not effectuated within a reasonable time period, specified by the party requesting the cure, such party shall terminate the contract, if feasible, or if not feasible report the problem to the Secretary of HHS or its designee. (See 45 C.F.R. § 164.504(e)(1)(ii) and HITECH Act § 13404(b)).
5. **Inspection of Books and Records.** **Business Associate** shall make available for inspection its internal practices, books, and records (relating to its use and disclosure of the PHI it creates for, or receives from, **Covered Entity**) to **Covered Entity** and/or the HHS to determine compliance with the HIPAA Regulations or the **Business Associate's** compliance with this agreement.
6. **Designated Record Set.** **Business Associate** agrees that all PHI received by or created for **Covered Entity** shall be included in an individual's Designated Record Set. **Business Associate** shall maintain such Designated Record Set with respect to services provided to an individual under this agreement and shall allow such individual to access the Designated Record Set as provided in the HIPAA Regulations.
7. **Restriction Contracts and Confidential Communications.** **Business Associate** shall comply with any agreement that **Covered Entity** makes that either; (i) restricts use or disclosure of PHI pursuant to 45 C.F.R. § 164.522(a); or (ii) requires confidential communication about PHI pursuant to 45 C.F.R. § 164.522(b), provided that **Covered Entity** notifies **Business Associate**, in writing, of the restriction or confidential communication obligations that **Business Associate** must follow. **Covered Entity** will promptly notify **Business Associate** in writing of the termination of any such restriction agreement or confidential communication requirement, and with respect to termination of any such restriction agreement, instruct **Business Associate** whether any PHI will remain subject to the terms of the restriction agreement.
- D. **Termination and Continuing Privacy and Security Obligations**
1. **Termination of Contract.** As required by the HIPAA Regulations and this agreement, **Covered Entity** may, in addition to other available remedies, terminate the contract if **Business Associate** has materially breached any provision of this agreement and has failed to cure or take actions to cure such material

breach within five (5) calendar days of such breach. **Covered Entity** shall exercise this right to terminate the contract by providing **Business Associate** written notice of termination, which shall include the reason for the termination. Any such termination shall be effective immediately or at such other date specified in **Covered Entity's** notice of termination. Within thirty (30) calendar days of such termination of the contract, **Business Associate** shall provide to **Covered Entity** one final report of any and all breaches made of all individuals' PHI during the term of the contract.

2. **Obligations upon Termination.** Upon termination, cancellation, expiration, or other conclusion of the contract, **Business Associate** shall:
 - a. As directed by **Covered Entity**, **Business Associate** shall immediately return or destroy all PHI, including all copies of and any data or compilations derived from, and allowing identification of, any individual who is a subject of the PHI, in whatever form or medium (including in any electronic medium under **Business Associate's** custody or control), and at whatever location the PHI resides including offices local and remote, data centers, remote storage facilities, off-site backup facilities and vendors, and all other locations, that **Business Associate** created or received for or from **Covered Entity**. Returned PHI must be provided to the **Covered Entity** in a common, nonproprietary, industry standard data format.
 - b. Complete all such return or destruction activities as promptly as possible, but no later than thirty (30) calendar days after the effective date of the termination, cancellation, expiration, or other conclusion of the contract.
 - c. These provisions shall apply to PHI that is in the possession of subcontractors or agents of **Business Associate**.
3. **Continuing Privacy and Security Obligation.** **Business Associate's** obligation to protect the privacy and security of the PHI, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI it created for or received from **Covered Entity**, shall be continuous and survive termination, cancellation, expiration, or other conclusion of the contract.
4. **Termination for Cause.** Without limiting the termination rights of the parties pursuant to the contract and upon **Covered Entity's** knowledge of a material breach of this contract by **Business Associate**, **Covered Entity** shall either:
 - a. Provide an opportunity for **Business Associate** to cure the breach or end the violation and, if **Business Associate** does not cure the breach or end the violation within the time specified by **Covered Entity**, terminate the contract, if feasible; or
 - b. Immediately terminate the contract if cure is not possible, if feasible.
5. **Effect of Termination.**
 - a. Except as provided in paragraph (2) of this Section, upon termination of the contract for any reason, as directed by **Covered Entity**, **Business Associate** shall promptly return or destroy all PHI received from or created or received by **Business Associate** on behalf of, **Covered Entity** that **Business Associate** maintains in any form and retain no copies. This provision shall apply to PHI that is in the possession of subcontractors or agents of **Business Associate**. Returned PHI must be provided to the **Covered Entity** in a common, nonproprietary, industry standard data format.
 - b. In the event that **Business Associate** reasonably believes that returning or destroying the PHI is infeasible, **Business Associate** shall provide to **Covered Entity** prompt notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return, or destruction is infeasible, **Business Associate** shall extend the protections of the contract to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as **Business Associate** maintains such PHI.

E. Conflicts

The terms and conditions of this agreement shall prevail in the event any terms and conditions herein conflict with any provision of the contract.

F. Privacy and Security Contact Information

1. Privacy

a. Covered Entity

- i. Attn: _____
- ii. Phone: _____
- iii. E-mail: privacyofficial@alaska.gov

b. Business Associate

- i. Attn: _____
- ii. Phone: _____
- iii. E-mail: _____

2. Security

a. Covered Entity

- i. Attn: _____
- ii. Phone: _____
- iii. E-mail: doh.its.dso@alaska.gov

b. Business Associate

- i. Attn: _____
- ii. Phone: _____
- iii. E-mail: _____

Covered Entity

Business Associate

Signature: _____

Signature: _____

By: _____

By: _____

Title: _____

Title: _____

Date: _____

Date: _____